DEPARTMENT OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

6.033—Computer System Engineering Handout 19—March 23, 1995

More on Satan, and The Manchurian Printer

This handout contains two new readings. The first one contains the last breaking news related to Satan. The second one is the Manchurian printer.If you saw the movie The Manchurian Candidate you will understand the reference in the title of the attached article, another late-breaking contribution to the current topic of security and privacy.

The first reading is two news articles that appeared in the San Francisco Chronicle and the New York Times:

1. FREEDOM ISSUE COSTS INTERNET EXPERT HIS JOB, by MICHELLE QUINN c.1995 San Francisco Chronicle
2. DISMISSAL OF SECURITY EXPERT ADDS FUEL TO INTERNET DEBATE, by JOHN MARKOFF, c.1995 N.Y. Times News Service

Reprinted 3/22/95 without permission, under the copyright law exception for timely use for educational purposes.

The second reading is:

The Manchurian Printer
Simson L. Garfinkel
The Boston Sunday Globe, March 5, 1995, Focus Section, Page 83
Also posted to RISKS-FORUM Digest 16, 92 (Thursday, 16 March 1995)
Reprinted with permission of the author.

3/21/95 7:41 PM Inches: 10.9 REGULAR BC_SATAN_QUITS_SFCHRON_03-21 0461

BC-SATAN-QUITS-SFCHRON

FREEDOM ISSUE COSTS INTERNET EXPERT HIS JOB By MICHELLE QUINN c.1995 San Francisco Chronicle

Dan Farmer, who grabbed the limelight in the technology world with his computer security program SATAN, and his big high-tech employer Silicon Graphics, have called it quits.

Citing philosophical differences, Farmer who wants to give his latest security program to all - crooks and corporations alike - lost his job yesterday at the Mountain View-based company.

"It's over," Farmer said in an interview yesterday over his cellular phone after he left the Silicon Graphics office. "The main issue is that I'm all for the free distribution of the program and they weren't. Being around me was a little hard for them."

The program, developed with his partner, Wietse Venema, a researcher at Netherlands University of Eindhoven, is set to be released April 5, Farmer's 33rd birthday. It will act like an X-ray on computer systems and networks, pinpointing all security weaknesses.

But the bug in Farmer's relationship with SGI is his plan to give the program away free over the Internet.

Bill Kelly, vice president of business development for SGI, said Farmer's departure was a mutual decision. The company was concerned Farmer would spend too much time dealing with the program and handling press calls. But primarily, they agreed, the disagreement was over Farmer's intention to give the program away.

"We feel strongly about security systems and we're concerned about the harm Dan's program will cause in the wrong hands," Kelly said. Farmer says he understands the company's views but could not change plans to distribute the program.

"I don't want to distribute things to harm people but my software can be used for gain," he said.

With the program, anyone can find the security weaknesses of a computer system, even if they are physically thousands of miles away. Programs similar to SATAN, which stands for Security Administrators Tool for Analyzing Networks, exist, but they are sold commercially for high prices.

Farmer says there may be some break-ins and crimes because of SATAN but in the long run computer systems worldwide will be stronger for the bitter medicine.

In December, Silicon Graphics hired Farmer knowing he was working on a security program. But they didn't not know he was planning to give it away.

Already, Farmer said he is fielding threatening calls from executives all over the world. "They say, 'If your program lays one electronic finger on my system, I'll sue you for everything you are worth.'

"I like to be thought of as a nice guy," he said. "That's why I'm making it free."

(For use by New York Times News Service clients)

3/21/95 7:05 PM Inches: 19.3 URGENT BC_SECURITY_SOFTWARE_DIS_ 03-21 0817

BC-SECURITY-SOFTWARE-DISPUTE-NYT

DISMISSAL OF SECURITY EXPERT ADDS FUEL TO INTERNET DEBATE

(EDS: Story embargoed until 10 p.m. ET.)

(th)

By JOHN MARKOFF

c.1995 N.Y. Times News Service

SAN FRANCISCO - Depending on your attitude toward Satan, a skilled computer security expert named Dan Farmer is either a genius or a menace.

Satan is a sophisticated software program, intended to find the security flaws in any computer system linked to the global Internet. Farmer helped create Satan and plans to begin distributing it free over the Internet early next month. He sees its dissemination as a public service to computer administrators who want to identify the chinks in their security armor so they can fix them.

But his employer, Silicon Graphics Inc., sharing the worries of many in cyberspace, fears that Farmer is about to put a powerful jimmy into the hands of hackers everywhere. So, on Monday, Silicon Graphics dismissed him.

The sacking of Farmer, who helped develop Satan on his own time, adds fuel to a controversy that has swirled around him in recent weeks as he has ignored the threat of lawsuits and various other forms of pressure to keep Satan on a short leash.

In the Internet community, Farmer's case is seen as symbolizing the conflict between a time-honored ideal - the free flow of information in cyberspace - and the harsh new reality that corporations and government agencies must protect their computer systems against intruders and vandals armed with increasingly sophisticated break-in software.

"This is the classic double-edged sword," said Peter Neumann, a computer scientist at SRI International, a research and consulting organization in Menlo Park, Calif.

"You have to get the information about how bad things are to people in order to fix the problems," Neumann said. "On the other hand, you run the risk of this information falling into the hands of sinister elements. So you lose either way because the systems aren't secure."

Farmer has his defenders, including some managers at Sun Microsystems Inc., the computer company where he worked as network security manager before taking a comparable job at Silicon Graphics in December.

Some executives at Sun Microsystems still think highly enough of Farmer that they would welcome him back. But Sun's lawyers see Farmer as a walking liability suit and are urging management to steer clear for the time being. They fear reprisals from government agencies, universities or corporations that may end up having their networks burglarized by Satan-wielding break-in artists.

"This lawyer's liability consciousness is exactly what the problem is," said John Gage, the director of the science office at Sun Microsystems. "The spirit of Dan Farmer's software is what we need to make complex computer systems secure."

Silicon Graphics, which has offered Farmer a severance package, said it had tried to be even-handed with him.

"We've been discussing this issue with Dan and we've agreed mutually that parting company at this time is appropriate," said William Kelly, the vice president of business development at Silicon Graphics. "It's fair to say that we at SGI did not agree with the distribution plan he has for that product."

Farmer said he understood, but disagreed with, Silicon Graphics.

"They're a corporation and they have to do what they have to do," he said.

But Farmer says he, too, must do what he has to do. "In a way, it's a freedom-of-speech issue," he said. "I want to teach people and have them learn about computer security."

Farmer said he had been developing Satan with a Dutch friend and colleague, Wietse Venema, and had intended all along to distribute it far, wide and free. It is scheduled to be released on April 5, Farmer's birthday.

The issue of whether little-known computer security flaws should be widely publicized has long been discussed among the computer experts who care for and maintain the computer hardware and software that make up the Internet.

One camp argues that the community of systems administrators who maintain computers is inherently lazy and will not make needed security changes unless forced to do so.

But other, more conservative, computer security workers are aghast at the prospect of an automated software tool like Satan being made available to anyone who wants to look for holes in computer network defenses. Freely distributing Satan, they contend, is like handing a loaded gun to every punk computer vandal in the world.

Whether he rejoins Sun Microsystems or is hired by another computer shop, Farmer could find the Satan controversy to be a career asset in the world of computer security.

"I've had people at a number of companies say they would love to hire me," he said. "But they said they weren't interested until April 6."

The Manchurian printer, (C) 1995, Simson L. Garfinkel

Simson L. Garfinkel

Early this month, Hewlett-Packard announced a recall of 10,000 HP OfficeJet printer fax copiers. The printer's power supplies may have a manufacturing defect that could pose an electrical shock hazard. HP says that it discovered the problem with its printers during routine testing; HP was lucky: printers can be very dangerous devices. A typical laser printer, for example, can draw hundreds of watts of power, generate internal temperatures high enough to burn a wayward human hand, and even, under the right circumstances, start a fire.

Most manufacturers, of course, try to design their printers to minimize such risks. Increasingly, however, there is a chance that companies might intentionally design life-threatening flaws into their products so that the flaws can be exploited at a later time. These fatal flaws might be intentionally built into equipment manufactured overseas, as a kind of “insurance policy" in the event of a war between that foreign country and the United States. The flaws might form the basis for a new kind of corporate warfare. Or the flaws might be hidden by disgruntled employees contemplating extortion or revenge.

Indeed, U.S. military planners are increasingly worried about this sort of possibility, they place under a heading "Information Warfare." Nevertheless, although the threat of Information Warfare is very real, an even bigger danger is that the Department of Defense will use this threat to convince the new Congress to repeal the Computer Security Act of 1987. This would effectively allow the National Security Agency to declare martial law in cyberspace, and could place the civilian computer industry into a tailspin.

To understand what the military is afraid of, imagine the Manchurian Printer: a low-cost, high-quality laser printer, manufactured overseas, with built-in secret self-destruct sequence. For years these printers could lay dormant. But send them a special coded message---perhaps a long sequence of words that would never normally be printed together---and the printer would lock its motors, overheat, and quickly burst into flames. Such an attack might be the first salvo in an out-and-out war between the two countries. Alternatively, an enemy company might simply use printers to start selective fires, damage economic competitors, take out key personnel, and cause mischief.

Unlike the movie the Manchurian Candidate, the technology behind the Manchurian Printer isn't science fiction. Last October, Adobe accidentally shipped a "time bomb" in Photoshop version 3.0 for the Macintosh. A time bomb is a little piece of code buried inside a computer program that makes the software stop running after a particular date. Adobe put two time bombs into its Photoshop 3.0 program while the application was under development. The purpose behind the time bombs was to force anybody who got an advance, pre-release copy of the program to upgrade to the final shipping version. But when it came time to ship the final version of Photoshop 3.0, Adobe's engineers made a mistake: they only took out one of the bombs.

An engineer inside Adobe learned about the problem soon after the product was shipped, and the company quickly issued a recall and a press release. Adobe called the time bomb a "security code time constraint" and said that "although this is an inconvenience to users, the security constraint neither damages the program or hard drive, nor does it destroy any files."

It only takes a touch of creativity and a bit of paranoia to think up some truly malicious variants on this theme. Imagine that a company wants to make a hit with its new wordprocessor: instead of selling the program, the company gives away free evaluation copies that are good for one month.
What's unknown to the users of this program is that while they are typing in their letters, the program is simultaneously sniffing out and booby-trapping every copy of Microsoft Word and WordPerfect that it finds on your system. At the end of the month, all of your wordprocessors stop working: Instead of letting you edit your memos, they print out ransom notes.

Any device that is equipped with a microprocessor can be equipped with such a booby-trap. Radios, cellular telephones, and computers that are connected to networks are particularly vulnerable, since an attacker can send them messages without the knowledge or consent of their owners. Some booby- traps aren't even intentional. What makes them particularly insidious is that it is almost impossible to look at a device and figure out if one is present or not. And there is no practical way to test for them, either. Even if you could try a million different combinations a second, it would take more than 200 years to find a sequence that was just 8 characters long.

* * *

Information Warfare isn't limited just to things that break or go boom. The Department of Defense is also worried about security holes that allow attackers to break into commercial computers sitting on the Internet or take over the telephone system.

"This nation is under IW attack today by a spectrum of adversaries ranging from the teenage hacker to sophisticated, wide-ranging illegal entries into telecommunications networks and computer systems," says a report of the Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield, and issued last October by the Office of the Secretary of Defense.

"Information Warfare could pervade throughout the spectrum of conflict to create unprecedented effects. Further, with the dependence of modern commerce and the military on computer controlled telecommunication networks, data bases, enabling software and computers, the U.S. must protect these assets relating to their vulnerabilities," the report warns.

Information warfare changes the rules of war fighting, the report warns. A single soldier can wreak havoc on an enemy by reprogramming the opposing side's computers. Modern networks can spread computer viruses faster than missiles carrying biological warfare agents, and conceivably do more damage. Worst of all, the tools of the information warrior are readily available to civilians, terrorists and uniformed soldiers alike, and we are all potential targets.

Not surprisingly, the unclassified version of the Pentagon's report barely mentions the offensive possibilities of Information Warfare---capabilities that the Pentagon currently has under development. Nevertheless, these capabilities are alluded to in several of the diagrams, which show a keen interest by the military in OOTW---Operations Other Than War.

"They have things like information influence, perception management, and PSYOPS---psychological operations," says Wayne Madsen, a lead scientist at the Computer Sciences Corporation in northern Virginia, who has studied the summer study report. "Basically, I think that what they are talking about is having the capability to censor and put out propaganda on the networks. That includes global news networks like CNN and BBC, your information services, like CompServe and Prodigy," and communications satellite networks. "When they talk about 'technology blockade,' they want to be able to block data going into or out of a certain region of the world that they may be attacking."

The report also hints at the possibility of lethal information warfare. "That is screwing up navigation systems so airplanes crash and ships runs aground. Pretty dangerous stuff. We could have a lot of Iranian Airbuses crashing if they start screwing that up," Madsen says. Indeed, says Madsen, the army's Signal Warfare center in Warrenton, Virginia, has already invited companies to develop computer viruses for battlefield operations.

Our best defense against Information Warfare is designing computers and communications systems that are fundamentally more secure. Currently, the federal organization with the most experience in the field of computer security is the National Security Agency, the world's foremost spy organization. But right now, NSA's actions are restricted by the 1987 Computer Security Act, which forbids the agency from playing a role in the design of civilian computer systems. As a result, one of the implicit conclusions of the Pentagon's report is to repeal the 1987 law, and untie the NSA's hands. Indeed, the Pentagon is now embarking on a high-level campaign to convince lawmakers that such a repeal would be in the nation's best interests.

This argument confuses security with secrecy. It also ignores the real reasons why the Computer Security Act was passed in the first place.

In the years before the 1987 law was passed, the NSA was on a campaign to expand its power throughout American society by using its expertise in the field of computer security as a lever. NSA tried to create a new category of restricted technical information called "national security related information." They asked Meade Data Corporation and other literature search systems for lists of their users with foreign-sounding names. And, says David Banisar, a policy analyst with the Washington-based Electronic Privacy Information Center, "they investigated the computers that were used for the tallying of the 1984 presidential election. Just the fact that the military islooking in on how an election is being done is a very chilling thought. After all, that is the hallmark of a banana republic."

The Computer Security Act was designed to nip this in the bud. It said that standards for computer systems should be set in the open by the National Institute of Standards and Technology.

Unfortunately, the Clinton Administration has found a way to get around the Computer Security Act. It's placed an "NSA Liaison Officer" four doors down from the NIST director's office. The two most important civilian computer standards to be designed in recent years---the nation's new Escrowed Encryption Standard (the "Clipper" chip) and the Digital Signature Standard were both designed in secret by the NSA. The NSA has also been an unseen hand behind the efforts on the part of the Clinton Administration to make the nation's telephone system "wiretap friendly."

Many computer scientists have said that the NSA is designing weak standards that it can circumvent, so that the nation's information warfare defenses do not get in the way of the NSA's offensive capability. Unfortunately, there's no way to tell for sure. That's the real problem with designing security standards in secret: there is simply no public accountability.

In this age of exploding laser printers, computer viruses, and information warfare, we will increasingly rely on strong computer security to protect our way of life. And just as importantly, these standards must be accountable to the public. We simply can't take our digital locks and keys from a Pentagon agency that's saying "trust me."

But the biggest danger of all would be for Congress to simply trust the administration's information warriors and grant their wishes without any public debate. That's what happened last October, when Congress passed the FBI's "Communications Assistance for Law Enforcement Act" on an unrecorded voice vote. The law turned the nation's telephone system into a surveillance network for law enforcement agencies, at a cost to the U.S. taxpayer of $500 million.

=========WHAT FOLLOWS ARE CAPTIONS FOR THE ART===========
Photo: Box of Microsoft Word 6.0

Even though it's illegal, a lot of people like to "try out" software by making a copy from a friend before they plunk down hundreds of dollars for their own legal copy. Computer companies say that this is a form of software piracy: many who try never buy. More than 2 billion dollars of software is pirated annually, according to the Business Software Alliance.

One way that companies like Microsoft and Novel could fight back is by booby-trapping their software. Sure, customers wouldn't like it if that stolen copy of Microsoft Word suddenly decided to erase every letter or memo that they've written in the past month, but what legal recourse would they have?
=====================
Photo: Cellular Telephone

Is your cellular phone turned on? Then your phone is broadcasting your position every time it sends out its electronic "heartbeat." Some law enforcement agencies now have equipment that lets them home in on any cellular telephone they wish (similar technology was used recently to catch infamous computer criminal Kevin Mitnick). Perhaps that's the reason that the Israeli government recently ordered its soldiers along the boarder to stop using their cellular telephones to order late night pizzas: the telephone's radio signal could be a become a homing beacon for terrorist's missiles.

===================

Photo: Floppy Disk

Beware of disks bearing gifts. In 1989, nearly 7000 subscribers of the British magazine PC Business World and 3500 people from the World Health Organization's database received a disk in the mail labeled "AIDS Information Introductory Diskette Version 2.0". People who inserted the disks into their computers and ran the programs soon found out otherwise: the disks actually contained a so-called trojan horse that disabled the victims' computers and demanded a ransom.

==================

Photo: A computer with a screen from America Online, and a modem

Several years ago, users of Prodigy were shocked to find that copies of documents on their computers had been copied into special "buffers" used by Prodigy's DOS software. Prodigy insisted that the copied data was the result of a software bug, and it wasn't spying on its customers. But fundamentally, if you use a modem to access America Online, Prodigy or Compuserve, there is no way to be sure that your computer isn't spying on you while you surf the information highway.

==================

HP's recall affects only OfficeJet printers with serial numbers that begin US4B1-US4B9, US4C1-US4C9, US4BA-US4BU, or US4CA-US4CK. Worried about your OfficeJet? Call HP at (800) 233-8999.

===============

Simson L. Garfinkel writes about computers and technology from his home in Cambridge, Massachusetts.